

# Internet Security for Small Businesses

## *Firewall Protection for the Small Business Network*

### Finding Security in the Ultimate Open Space

Network administrators have good reason to feel beleaguered today. Amid well-publicized attacks on the world's most sophisticated and best-designed networks, IT managers must somehow keep their own networks safe and their companies' private data secure. At the same time they face an overwhelming demand for new communication services, many of them delivered over the public Internet.

In fact the Internet has become an irreplaceable tool for most businesses. It is the primary source of market news and competitor intelligence, a conduit to customers, a medium of direct commerce, and an essential tie to partners and suppliers. Increasingly, it is even being used to extend the traditional WAN.

But when a private network connects to the Internet, it opens physical links to more than 50,000 unknown networks and all their unknown users. While this interconnectedness brings exciting opportunities for information sharing, it also brings threats to information not meant for sharing. Network managers face the task of giving their organizations the connectivity they need for corporate and individual communications, while keeping their sensitive information and proprietary data secure. The good news is that with planning, discipline and a modest investment, secure operation over the Internet is possible for businesses of any size.

### First Line of Defense: The Firewall

The primary means of securing a private network against penetration from a public one is a firewall. Simply put, a firewall is an access control device, performing perimeter security by deciding which packets are allowed or denied, and which must be modified before passing. When implemented as part of a comprehensive security policy, a firewall can provide effective defense against unauthorized access by external users.

The challenge with firewalls is getting the right amount of security without imposing unacceptable limitations on internal users or undue management complexity. This paper reviews the most common types of external threats, conventional firewall solutions, and the simpler, more flexible systems replacing them.

### Benefits of a Firewall

In addition to access control, an Internet firewall provides a natural focal point for the administration of other network security measures. A firewall can monitor all traffic entering and leaving the private network, and alert the IT staff to any attempts to circumvent security or patterns of inappropriate use. It can also provide Network Address Translation (NAT), a service that re-addresses data packets as they pass the firewall. This not only simplifies address management by allowing a single external address to be used for all internal users; it masks the true addresses of internal computers and servers from prying eyes outside.

A perimeter firewall also makes an ideal location for outward-facing resources such as Web and FTP servers. A firewall can be configured to allow Internet access to these systems while blocking or filtering admission to other, protected resources.

## Methods of Attack

To better understand the benefits a secure firewall can bring to a network, it's useful to know something about the most common types of attacks. Hackers vary widely in both motivation and skill. Some pursue specific information for profit, others seek control of computing and communication systems for their own use. Many, unfortunately, regard hacking as entertainment and justify vandalism as proof of their successful access.

Whatever the motivation, attacks that aim to penetrate a network often begin with surveillance to map the target network, collect user and host system information and probe for security weaknesses. Much of this intelligence gathering is conducted with widely available tools that were, ironically, designed to help network engineers evaluate and improve security.

- *Port Scans, Ping Sweeps, E-mail Recon and DNS High Zone Transfers* are just a few common techniques for probing a network to learn what systems are active, what services they offer, and what security measures are in place. If security is lax, simple probes can even disclose user account information.
- *Packet Sniffers* are reconnaissance programs used once a network host has been compromised, to capture and divert data packets for analysis. Used by an authorized technician they provide useful information about network utilization and efficiency. Used by a hacker, sniffers can reveal user names, passwords, system addresses, and even allow unencrypted messages to be read. Numerous freeware and shareware packet sniffers are widely available that allow relatively unskilled saboteurs to collect extensive information with which to mount an attack.

Armed with sufficient information about the layout of a network, its defenses and its users, an attacker will often attempt to gain access to thinly defended systems, acquire additional information and exploit an initial opening to infiltrate other systems.

Depending on his motivation and level of skill, an intruder may attempt to steal or destroy data, divert network assets for his own use (long distance telephone service, for instance), or simply disable the network. Common types of attacks include:

- *IP Spoofing* is the use of an internal address to mask the true source of an external transmission.
- *Application-Level Attacks* are assaults aimed at the server software running specific network services like e-mail. Often these attacks take advantage of security loopholes in older software versions, allowing an intruder to take control of the service, or even the server itself.
- *Trojan Horse Attacks* use camouflaged software to trick users or systems into providing useful information or lowering security barriers. A classic example is a substitute network login that prompts users to enter their user name and password, then sends that information to a hacker. The "I Love You" and "Melissa" e-mail attacks are among recent Trojan Horse variations. Others include Java applets and ActiveX controls embedded in web pages so as to execute when an apparently harmless page is transmitted. These attacks are particularly virulent because the platform independent nature of the programming languages allows them to spread to any and all connected systems.
- *Denial of Service Attacks* like SYN flooding, take advantage of network communication protocols to flood a host with incomplete requests for service, blocking legitimate inquiries.

## Four Types of Firewalls

A firewall is an access control system that analyzes all data traffic entering and leaving a private network, and allows or blocks passage based on security policies predefined by system administrators. Its core functions include high-volume packet inspection, internal address masking and hazardous content detection. In addition, the firewall itself must be resistant to attack so hackers can't penetrate the network by simply taking control of the firewall.

It is important to understand that a firewall can be only as effective as the security policy it enforces. Without a well-documented security program supported by an informed user group, no network can be reliably protected. In addition, a firewall cannot protect against threats that bypass the network interface, a virus-infected floppy disc, for instance. A comprehensive security policy must address all possible sources of harm and enlist all users in the security effort.

*Basic Router Security*—Elementary security measures are built in to most current access routers, including Access Control Lists (ACLs) and Network Address Translation (NAT). ACLs are lists of permitted and prohibited addresses that allow transmissions to be accepted or rejected based on their origin or destination. NAT is an address exchange that allows multiple private internal addresses to be mapped to a single public address. This effectively conceals the true identity of internal systems and prevents attackers from addressing them directly.

*Packet Filtering Firewalls*—The next level of firewall security is defined by packet filtering firewalls. These are systems capable of inspecting data packets based on a more complex rule base. Access rules can address any of the values included in the header portion of a data packet, including the source and destination addresses, source and destination ports, and message protocol type among others. While packet filtering allows more fine-grained security, configuring access rules requires a detailed knowledge of network services and communication protocols, and complicated rule sets can degrade routing performance. In addition, filtering rules based solely on header information provide no way to address higher-level security issues related to specific services.

*Stateful Inspection Firewalls*—A simpler, yet more rigorous method of access control analyzes packets in terms of sessions. If an incoming transmission appears to be a legitimate reply to a previous request from inside the network, the firewall allows it to pass. This approach allows relatively unrestricted transmission from inside the network, and selective, but flexible access from the outside. In conjunction with simple ACLs, stateful inspection provides easily administered protection that requires substantially less processing power at the firewall. An even more secure type of stateful inspection uses a monitoring algorithm to track individual connections and open temporary “doors” in the firewall under appropriate conditions. Packets are allowed to pass only if associated with a valid session initiated from within the network.

*Application Level Gateways*—Also known as proxy servers, application level gateways are firewalls designed to protect specific network services by restricting the features and commands that can be accessed from outside the network. Lightweight proxy applications running on the firewall mimic internal services and present reduced feature sets to external users. Because the proxy service interposes itself between users and vulnerable services, no direct contact occurs, greatly reducing the possibility of external attack. If no proxy service is installed for a network service, no external access is permitted. While application level firewalls provide a greater degree of security than packet filters, it comes at the cost of greatly increased processing loads at the firewall and reduced convenience for internal users.

### Three Ways to Implement Firewalls

The four approaches to firewall design described above have distinctly different hardware and software requirements, each with its own implications for the capital cost, manageability, user friendliness and ultimate security of the firewall system.

*Integrated or Router Based Firewalls*—Many access routers offer firewall capabilities as software-based additions to their basic security features. Used in this way, the router’s processor and memory are shared between routing and firewall functions. Both packet filtering and stateful inspection firewalls are available as router-based solutions. This is typically the most cost-effective means of establishing firewall protection.

*Proxy Server Firewalls*—In order to accommodate the higher processing loads associated with multiple proxy applications running concurrently, application level gateways are usually hosted on either a dedicated PC or server. The greater hardware cost is reflected in the generally higher overall cost of proxy firewalls, as is the need for client software if the security system is to be made transparent to internal users. Further considerations with proxy firewalls include lower routing speeds than those delivered by dedicated routers, and the vulnerability of the most popular PC and server operating systems. Because these systems and their security weaknesses are widely understood, they are more difficult to insulate from attack.

*Dedicated Firewall Appliances*—Standalone firewall appliances are specialized devices optimized for firewall performance, scalability, and security. Often they feature proprietary operating systems specifically designed to frustrate attacks. Because these are single purpose systems, the total cost of a dedicated firewall may be higher than an integrated solution, but they offer a clear advantage when high throughput is required and the most stringent security is warranted.

## Cisco Security Solutions: Firewall Protection for Every Business

As the leading supplier of infrastructure technology for corporate networks and the Internet, Cisco offers a full range of secure access solutions tailored for small to medium-sized businesses, designed to provide reliable data networking and to support fully integrated data and communication services. Both router-based firewall solutions and dedicated firewall appliances are available to fit the capacity needs and budgets of the smallest home office or the largest enterprise network

*Cisco Integrated Firewall Solutions* are dual-purpose systems that combine high performance Cisco access routers with firewall features of Cisco IOS® Software. Router-based integrated firewalls provide multiprotocol routing, stateful firewall protection, and a secure platform for virtual private network (VPN) deployment. They offer growing businesses an efficient, flexible, and highly scalable solution to the problems of connection security.

*Cisco Modular Access Routers*, the hardware portion of an integrated firewall solution, deliver reliable, secure connection to the Internet, LAN, and corporate WAN over DSL, cable, ISDN, or serial (T1, Frame Relay, leased lines). Their modular design provides an ideal platform for immediate voice and data connectivity with built-in support for full voice/data and fax integration. Solutions are available for every size business:

*800 Series*—small office/home office and corporate telecommuter


*1700 Series*—small business, mid-size, and small branch office

*2600 Series*—medium-sized business

*Cisco IOS Software*, the operating system on all Cisco routers, provides the intelligence behind the Internet and the firewall capabilities in router-based, integrated firewall solutions. *Cisco IOS Firewall Software*, an optional feature set specifically for integrated firewall applications, enriches the basic security capabilities of IOS software with context-based access control (CBAC), a connection-oriented stateful packet inspection system. CBAC creates dynamic access control lists in response to outbound messages from the internal network. Inbound packets from addresses that correspond to the destination of outbound messages are allowed to pass. Inbound packets that cannot be associated with an existing connection are blocked and discarded. Context-based inspection provides reliable network security in a simple, flexible, easily administered package. Other features of Cisco IOS Firewall Software include:

- Intrusion detection
- Authentication proxy
- Denial of service detection and prevention
- Controlled downloading of Java applets
- Real-time alerts
- TCP/UDP transaction log
- Dynamic port mapping
- VPN support via IPSec, L2TP, L2F, and GRE tunneling for low-cost, secure, encrypted communication over public networks
- Configuration and management systems

*Cisco Secure PIX Firewalls* are dedicated firewall appliances that offer an unprecedented level of network security. As dedicated appliances they provide no WAN interfaces and support no routing protocols other than RIP. Installed between a WAN router and the internal network they provide sophisticated stateful access control based on Adaptive Security Algorithm (ASA), an exclusive session state monitoring technology. ASA tracks individual connections by packet source and destination addresses, TCP sequence numbers, port numbers, and other TCP packet flags. Packets are allowed through the firewall only if associated with a valid session initiated from within the network. This gives organizations transparent access for internal and authorized external users, while protecting internal networks from unauthorized access.



An additional security feature of PIX firewalls is a non-UNIX embedded operating system. This proprietary control software eliminates the vulnerabilities of a well-known, general-purpose operating system, and delivers stunning performance. The largest PIX firewalls are capable of maintaining up to 250,000 simultaneous connections without affecting end-user performance. For applications where rigorous security and high throughput are essential, Cisco PIX firewalls are the logical solution.

Cisco Secure PIX Firewall appliances are available for every size business:

*PIX 506*—High-end small office/home office

*PIX 515*—Small and medium-sized business and remote office

*PIX 520*—Enterprise and service provider

## Cisco Solutions in the Spotlight

Cisco and its worldwide network of value-added resellers have helped thousands of small and medium-sized businesses leverage the power of the Internet to slash communication infrastructure expense, expand commerce opportunities, improve customer service and reforge their supply chains.

*Adding firewall security to an existing access router*—“Advance Capital” is a new business incubator that provides funding, management consulting, administrative services and infrastructure support for start-up businesses. Until recently, no access control was implemented. Internal growth and an expanding customer support load prompted several improvements to the firm’s network, which were achieved through reconfiguration and software enhancements to an existing Cisco 1720 access router.

First, technicians configured Network Address Translation to provide up to 255 internal addresses and conceal a block of 30 public addresses that had previously been exposed. At the same time, they added Cisco IOS Firewall Software to the router’s IOS operating system to provide firewall protection.

Six months after the upgrade, the firm’s system administrator expresses complete satisfaction with the improvements. Speaking of the 1720 router firewall he says, “It just works.”

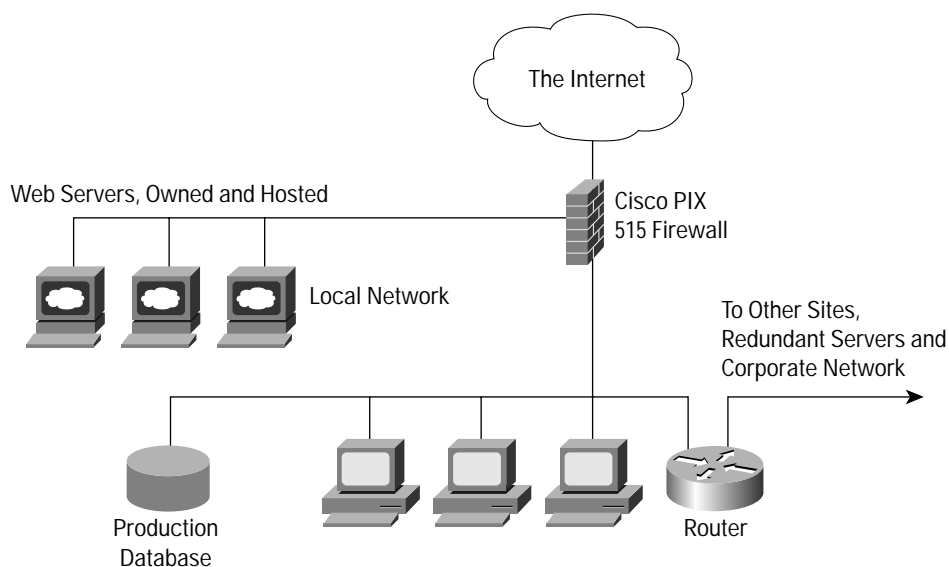
*Securing a new Web site*—“Fuel Services” is an oil and gas pipeline carrier that contracts with producers to transport well output to specified delivery points, typically refineries. As a division of “Carbon Corporation,” the firm’s Internet access was originally supplied over a corporate WAN.

In 1998, Fuel Services decided to create a Web service that would allow customers to access an internal database with real-time production information down to the level of individual wells. The service was a custom application developed on a Windows NT platform, accessing an existing Oracle database, and deployed on redundant servers in two company facilities.

Based on prior experience with Cisco systems in the company LAN, Fuel Services chose Cisco equipment for the Internet firewall, selecting PIX 515 firewalls for their high capacity and to take advantage of the additional security provided by the embedded operating system. The new Web servers were installed in secure subsections of the network, separated by the firewalls from both the public and internal networks, and T1 connections were established between the firewalls and ISP (Figure 1).

In eighteen months since the Web service went live, no security breaches have been detected and customer response to the improved reporting tool has been enthusiastic. In addition, the site’s success led to the installation of additional servers hosting applications for several other Carbon divisions, all behind the security of the original PIX firewalls.

Figure 1 "Fuel Services" Secure Network



## Come to Cisco for Small System Security Solutions

Cisco Systems provides the technology and the intelligence that makes the Internet and the world's largest enterprise networks possible, but that's just part of a much larger story. Cisco is also the leading developer of networking, access, and security solutions for small and medium-sized businesses. More than any other system supplier, Cisco has the tools and the experience small businesses need to ensure a larger future. For more information on Cisco firewall and network access solutions for your business please visit <http://www.cisco.com> for further information.



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems Europe  
11, Rue Camille Desmoulins  
92782 Issy Les Moulineaux  
Cedex 9  
France  
[www.cisco.com](http://www.cisco.com)  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems Australia, Pty., Ltd  
Level 17, 99 Walker Street  
North Sydney  
NSW 2059 Australia  
[www.cisco.com](http://www.cisco.com)  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

**Cisco.com Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE  
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia  
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore  
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 2000, Cisco Systems, Inc. All rights reserved. Printed in the USA. Access Registrar, AccessPath, Any to Any, Are You Ready, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, CiscoLink, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, Packet, PIX, Point and Click Internetworking, Policy Builder, Precept, RateMux, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Aironet, ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, CollisionFree, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0007R) 9/00 LW